United Nations A/70/127

General Assembly

Distr.: General
2 July 2015

Original: English

Seventieth session
Item 93 of the preliminary list*
Developments in the field of information and telecommunications in the context of international security

Note verbale dated 26 June 2015 from the Permanent Mission of Bangladesh to the United Nations addressed to the Secretary-General

The Permanent Mission of the People's Republic of Bangladesh to the United Nations in New York presents its compliments to the Secretary-General of the United Nations and, in its capacity as Chair of the Governing Council of the Inter-Parliamentary Union, has the honour to forward herewith to the General Assembly the text (in English and French) of the resolution entitled "Cyberwarfare: a serious threat to peace and global security", adopted by the 132nd Assembly of the Inter-Parliamentary Union, held in Hanoi on 31 March 2015 (see annex).

The Permanent Mission of the People's Republic of Bangladesh to the United Nations kindly requests the Office of the Secretary-General to circulate the present note verbale and its annex as a document of the seventieth session of the General Assembly, under item 93 of the preliminary list.

* A/70/50.

15-11167 (E) 130715

Please recycle

Annex to the note verbale dated 26 June 2015 from the Permanent Mission of Bangladesh to the United Nations addressed to the Secretary-General

[Original: English and French]

Cyberwarfare: a serious threat to peace and global security

Resolution adopted by consensus* by the 132nd Assembly of the Inter-Parliamentary Union (Hanoi, 1 April 2015)

The 132nd Assembly of the Inter-Parliamentary Union (IPU),

Mindful that information and communications technologies (ICTs) are means of inclusion and development and must not be used by States or non-State actors to violate international law, in particular the provisions and principles of the Charter of the United Nations relating to sovereignty, non-intervention, the sovereign equality of States, the peaceful settlement of disputes and the prohibition of the threat or use of force,

Acknowledging the work accomplished by the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security,

Considering that people's access to cyberspace involves, inter alia, extensive digital communication via satellites, optical networks and advanced computer programs, the systematic exchange of information, graphic, audiovisual and computerized data, intelligent tools and equipment, software, advanced operating systems and the possibility to use them for their own purposes,

Acknowledging that improper use of technology can have a harmful impact at national, regional and even global levels, and that internationally applicable legal regulatory authorities and instruments must therefore be established with regard to its purpose and use,

Convinced that, given the immense socioeconomic benefits that cyberspace brings to all citizens around the world, predictability, information security and stability in the cyberdomain are essential,

Having considered United Nations General Assembly resolutions 31/72 of 10 December 1976 (on a convention on the prohibition of military or any other hostile use of environmental modification techniques), 55/63 of 4 December 2000 and 56/121 of 19 December 2001 (on combating the criminal misuse of information technologies), 69/28 of 2 December 2014 (on developments in the field of information and telecommunications in the context of international security) and 57/239 (on the creation of a global culture of cybersecurity),

Recognizing the importance of international and regional agreements on cybercrime, transnational organized crime, the exchange of information and administrative assistance, including the 1977 Convention on the Prohibition of Military or Any Other Hostile Use of Environmental Modification Techniques, the 2001 Council of Europe Convention on Cybercrime and its Additional Protocol (concerning the criminalization of acts of a racist and xenophobic nature committed

* The delegation of the Bolivarian Republic of Venezuela expressed a reservation on the use of the term "cyberwarfare".

through computer systems), the 2010 Arab Convention on Combating Information Technology Offences and the 2009 Shanghai Cooperation Organization Agreement on Cooperation in the Field of International Information Security; *also recognizing* the importance of international treaties in preventing cyberwarfare,

Fully aware that some concepts, definitions and standards of cyberpolicy, especially in cyberwarfare and as they relate to international peace and security, are not commonly understood and are still being clarified at the national, regional and international levels, and that international consensus still does not exist in some areas,

Welcoming the progress made in international forums towards a common perception of what constitutes acceptable behaviour on the part of States in cyberspace, in particular by the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security and by other bilateral, regional and multilateral initiatives,

Acknowledging that certain principles of public international law, including, in particular, those contained in the Charter of the United Nations, the 1949 Geneva Conventions and their Additional Protocols, the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights and the Convention on the Elimination of All Forms of Discrimination against Women, are relevant and applicable to cyberspace and are essential to maintaining peace and international stability and promoting an open, secure and peaceful ICT environment, accessible to women and men alike,

Considering that cyberspace is more than the Internet, that the use of hardware, software, data and information systems can have effects beyond networks and IT infrastructure and is considered as a tool of economic growth, and that inequalities, including gender inequalities, exist in the ICT environment,

Cognizant of the fact that different areas of cyberpolicy, while distinct, are inextricably linked and may have an impact on international peace and security aspects of cyberspace, and vice versa,

Considering that the covert and illegal use, by individuals, organizations and States, of the computer systems of foreign countries to attack third countries is a matter of grave concern because of its potential to spark international conflicts,

Also considering that cyberspace has the potential to be exploited as a new dimension of conflict as well as a new operating environment where many, if not most, cyberassets have both civilian and military applications,

Aware that cyberspace is not an isolated domain and that destabilizing activities within it may have serious effects on other areas of global social life, trigger other, traditional forms of insecurity or conflict, or start a new type of conflict, and *convinced* that there is a need for regional and international cooperation against threats resulting from the malicious use of ICTs,

Also convinced that States should encourage the private sector and civil society to play an appropriate role to improve the security and use of ICTs, including supply chain security for ICT products and services,

Aware that military ICT systems for the deployment and use of force are susceptible to acts of cyberwarfare that could lead to third parties intercepting and

deploying such systems to cause unauthorized, illegal and destructive use of force, *concerned* that fully autonomous military systems ("killer robots") are especially vulnerable to such unauthorized deployment, as there is no human validation of final targeting decisions, and *especially concerned* that the hacking of nuclear weapon command-and-control systems could result in the unauthorized launch and detonation of nuclear weapons and cause unparalleled catastrophes,

Noting that the use of ICTs has reshaped the national and international security environment and that such technologies can be used for malicious purposes and to violate human and civil rights; *also noting that*, in recent years, the risk of ICTs being used by State and non-State actors alike to commit crimes, including violence against women and girls, and to conduct disruptive activities has risen significantly,

Bearing in mind the negative impact that the unlawful use of ICTs could have on State infrastructure, national security and economic development, and *aware* that the only viable means of preventing and dealing with these new challenges, consolidating the positive aspects of ICTs, preventing their potential negative effects, promoting their peaceful and legitimate use and guaranteeing that scientific progress is aimed at maintaining peace and promoting the well-being and development of peoples is joint cooperation between States, which will also prevent cyberspace from becoming a theatre of military operations,

Considering that cyberwarfare may encompass, but is not necessarily limited to, operations against a computer or a computer system through a data stream as a means and method of warfare that is intended to gather intelligence for the purpose of economic, political or social destabilization or that can reasonably be expected to cause death, injury, destruction or damage during, but not exclusively in, armed conflicts,

Aware that cyberdefence and cybercrime control measures complement each other, and *noting*, in this connection, that the Council of Europe Convention on Cybercrime (Budapest Convention), the only international treaty on crimes committed via the Internet and other computer networks, is open for accession, including by third countries,

Noting that the military use of cyberspace and the impact of specific activities are not yet fully understood; *also noting* that many cyberactivities may have the effect of destabilizing the security situation, depending on their nature, range, potential consequences and other circumstances,

Concerned about the suggestion by military planners that nuclear deterrence be maintained as an option for dealing with the existential threat of a cyberattack,

Acknowledging that a lack of strategic State-to-State communications, prompt attribution of responsibility and a limited understanding of allies' and adversaries' priorities may lead to miscalculation, misconception and misunderstanding in the cyberdomain, and that it is therefore important to introduce confidence-building measures of a nature to improve transparency, predictability and cooperation between States,

Considering that the risk to international peace and security has increased with the development and spread of sophisticated malicious tools and techniques by States and non-State actors,

Rejecting States' use of cyberspace as a means of applying economic, restrictive or discriminatory measures against another State for the purpose of limiting access to information or services,

Condemning the use of ICTs in contravention of international law, the goals and principles of the Charter of the United Nations and internationally recognized rules of coexistence between States,

Also condemning the use of ICTs by criminal or terrorist groups to communicate, collect information, recruit, organize, plan and coordinate attacks, promote their ideas and actions and solicit funding, and *mindful* that, in so doing, these groups often exploit the vulnerability of certain social groups, and *further condemning* the use of cyberspace to destabilize and threaten international peace and security,

Noting the need to work for the conclusion of an international Internet convention to prevent the use of the Internet by terrorists or terrorist organizations for illegal activities, in particular to raise funds, enlist members or publish ideas inciting people to violence and hatred,

Recalling that acts of sexual violence during times of war or conflict are considered to be war crimes, and *considering* that the broadcast of such acts using ICTs to intimidate, threaten or terrorize citizens, communities or countries and force them into submission therefore constitutes a crime of cyberwarfare,

Considering that there is a need to strike a balance between security control of cyberspace and respect for privacy, confidentiality, intellectual property and e-government and e commerce development priorities,

Also considering that there is a need to develop national, regional and international levels of practical confidence-building measures in the ICT field,

Condemning any intentional misuse of technology, including, but not limited to, State sponsored espionage,

1. *Recommends* that parliaments build their capacities to better understand the complex nature of national and international security in the cyberdomain and to take into account the interlinkages between different areas of cyberpolicy development;

2. *Encourages* parliaments to work with other branches of government, civil society and the private sector to develop a holistic understanding of cyberdependence, risks and challenges at the national level; *further encourages* Governments to reduce the negative effects of cyberdependence, especially with regard to e-government development and national security, and to promote the adoption of national cybersecurity strategies;

3. *Calls upon* all parliaments to review their countries' legal framework to examine how best to adapt it to potential threats, in terms of crime, terrorism and/or warfare, which might arise from the evolving nature of cyberspace;

4. *Also calls upon* parliaments to legislate to counter acts of sexual violence against women and girls during times of war and conflict, which constitute war crimes, and against the broadcasting of such acts using ICTs, which is a crime of cyberwarfare;

5. *Encourages* parliaments to be accountable by scrutinizing public finances with a view to ensuring that adequate resources are allocated to cybersecurity;

6. *Also encourages* parliaments to make use of all the oversight tools at their disposal to ensure that cyber-related activities are rigorously monitored, and to enact national laws, with due regard for their respective constitutions, that stipulate stiffer penalties for cyberattacks, using appropriate safeguards, governance mechanisms and existing structures so as to protect freedom of expression and not compromise the citizen's ability to use ICT tools;

7. *Recommends* that parliaments from States which have not yet done so request that their respective Governments expressly state that international law, including the law of armed conflict, must apply to cyberwarfare in order to ensure that limits are placed on the use of cyberoperations as a means and method of warfare, while noting that the exact manner of application is still a matter under international discussion;

8. *Encourages* parliaments to work with other branches of government and with civil society to develop a comprehensive cybersecurity strategy encompassing cyberdefence, capacity-building and action to combat cyberterrorism;

9. *Invites* parliaments to support the dissemination of cybersecurity information and best practices among all national stakeholders;

10. *Calls upon* all parliaments to ensure meaningful participation by all stakeholders, including the private sector, academics, the technical community, civil society and women's organizations and associations, in efforts aimed at addressing the cyberthreats related to the use of ICTs;

11. *Recommends* that parliaments from nuclear-weapon States call on their Governments to rescind launch-on-warning policies, stand down nuclear weapons from high operational readiness and extend the decision-making time for nuclear-weapon use in order to prevent unauthorized activation and deployment of nuclear-weapon systems through cyberattacks, pursuant to the negotiation of agreements to prohibit the use of nuclear weapons and achieve their elimination;

12. *Calls upon* all parliaments to ensure that their national laws and regulations do not condone the criminal use of cybertechnology for the purpose of fomenting conflict between States or provide the perpetrators with immunity and a safe haven;

13. *Encourages* national parliaments to promote close cooperation and partnership between the public and private sectors, so as to improve the effectiveness of cybersecurity and cyberdefence strategies at the national level;

14. *Recommends* the application of a strategic information plan involving the education sector, organized communities and citizen participation, for the purpose of heightening awareness of the benefits and usefulness of being active in cyberspace and the harmful effects that can be generated from its misuse;

15. *Also recommends* that States comply with international law and the Charter of the United Nations when using ICTs and that, at the legislative and executive levels, consideration be given to cooperative measures likely to enhance peace and international stability and security and lead to a common understanding

of the application of the relevant international law and derived standards, rules and principles underpinning the responsible conduct of States;

16. *Encourages* parliaments to support the widest possible accession to the Council of Europe Convention on Cybercrime (Budapest Convention) as a means of strengthening national legislation and enhancing the effectiveness of international cooperation against cybercrime;

17. *Recommends* that parliaments press for the formulation and adoption at the regional and international levels of appropriate regulations and oversight guaranteeing that the use of cyberspace is fully compatible with international law, the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights and internationally recognized rules of coexistence, together with practical confidence-building measures to help increase transparency, predictability and cooperation and reduce misconceptions, thus diminishing the risk of conflict using the cyberdomain;

18. *Invites* parliaments to support the use of aid instruments and resources for capacity-building to prevent and counter cyberthreats;

19. *Urges* the IPU, together with relevant international organizations, to lend support to inter-parliamentary cooperation with a view to promoting international agreements guaranteeing better use of ICTs by countries and appropriate and secure use of cyberspace, to sharing good practices on confidence-building measures that are conducive to peace and international stability and security in that they reduce the security risks inherent in the use of ICTs, and to developing collaborative mechanisms;

20. *Encourages* parliaments to play a positive role in creating a secure environment in support of the peaceful use of cyberspace and ensuring that freedom of expression and information exchange are appropriately reconciled with public safety and security concerns;

21. *Also encourages* parliaments to work with their Governments on establishing international agreements to prevent cyberwarfare, apply the body of international peace and security law to cyberspace, establish global standards and ensure that national and international responses to cyberattacks are consistent with such agreements and standards;

22. *Further encourages* international cooperation to provide developing countries with technical assistance and capacity-building in terms of prevention, investigation and the prosecution and punishment of offenders, and to enhance network security in relation to cyberwarfare;

23. *Calls on* the IPU to urge the United Nations to adopt a resolution prohibiting illegal monitoring and cyberattacks on critical infrastructure such as water, electricity and hospital networks;

24. *Encourages* the United Nations to enhance cybersecurity by establishing a global registry of cyberattacks;

25. *Recommends* that the legal instruments, agreements and cooperation agreements, inter alia, relating to cyberspace, cybersecurity, technology and telecommunications be reviewed and updated;

26. *Suggests* that the IPU, acting on the basis of this resolution, propose that the General Assembly of the United Nations convene a conference on the prevention of cyberwarfare with a view to adopting a unified position on the issues involved and drafting an international convention on the prevention of cyberwarfare.